

What is claimed is:

Sub  
As

1. A method for filtering packets, comprising:
  - 2 receiving a packet sent from a first device to a second device;
  - 3 authenticating an identifier for said packet;
  - 4 determining whether to send said packet to said second device; and
  - 5 sending said packet to said second device in accordance with said
  - 6 determination.
2. The method of claim 1, wherein said determining comprises:
  - 2 comparing said identifier to a list of identifiers;
  - 3 retrieving at least one policy rule;
  - 4 determining whether to send said packet to said second device in accordance
  - 5 with said comparison and said policy rule.
3. The method of claim 1, wherein said identifier is a common host identifier.
4. The method of claim 1, wherein said authenticating is performed in accordance
  - 2 with IPSEC standards.
5. The method of claim 1, wherein said authenticating comprises:
  - 2 retrieving a pointer to a security association from an authentication header
  - 3 from said packet;
  - 4 retrieving a key associated with said security association; and
  - 5 determining whether said packet is authentic using said key.

1 6. The method of claim 5, wherein said identifier is not authentic, further  
2 comprising sending a first message to a third device indicating said identifier is not  
3 authentic.

1 7. The method of claim 5, wherein said authentication header is an IPSEC  
2 authentication header.

1 8. The method of claim 1, wherein said packet is encrypted prior to said  
2 receiving, further comprising decrypting said packet prior to authenticating.

1 9. The method of claim 8, wherein said packet is encrypted and decrypted using  
2 one of group of cryptographic techniques comprising DES, triple DES, HMAC and  
3 RSA.

1 10. The method of claim 1, wherein said policy rule is stored in a policy  
2 configuration file at said second device.

1 11. A machine-readable memory whose contents cause a computer system to  
2 perform packet filtering, by performing the steps of:  
3 receiving a packet sent from a first device to a second device;  
4 authenticating an identifier for said packet;  
5 determining whether to send said packet to said second device; and  
6 sending said packet to said second device in accordance with said  
7 determination.

A(

1 12. The machine-readable memory of claim 11, wherein said determining  
2 comprises:  
3 comparing said identifier to a list of identifiers;  
4 retrieving at least one policy rule;  
5 determining whether to send said packet to said second device in accordance  
6 with said comparison and said policy rule.

1 13. The machine-readable memory of claim 11, wherein said identifier is a  
2 common host identifier.

1 14. The machine-readable memory of claim 11, wherein said authenticating is  
2 performed in accordance with IPSEC standards.

1 15. The machine-readable memory of claim 11, wherein said authenticating  
2 comprises:  
3 retrieving a pointer to a security association from an authentication header  
4 from said packet;  
5 retrieving a key associated with said security association; and  
6 determining whether said packet is authentic using said key.

1 16. The machine-readable memory of claim 15, wherein said identifier is not  
2 authentic, further comprising sending a first message to a third device indicating said  
3 identifier is not authentic.

1 17. The machine-readable memory of claim 15, wherein said authentication header  
2 is an IPSEC authentication header.

1 18. The machine-readable memory of claim 11, wherein said packet is encrypted  
2 prior to said receiving, further comprising decrypting said packet prior to  
3 authenticating.

1 19. The machine-readable memory of claim 18, encrypted and decrypted using one  
2 of group of cryptographic techniques comprising DES, triple DES, HMAC and RSA.

1 20. The machine-readable memory of claim 11, wherein said policy rule is stored  
2 in a policy configuration file at said second device.

1 21. A packet filter for a distributed firewall, comprising:  
2 an input means coupled to said first network for receiving a data packet from a  
3 first device, said data packet having an encrypted common host identifier;  
4 a first buffer coupled to said input means for storing said received packet;  
5 a first memory segment containing a list of common host identifiers and at  
6 least one policy rule;  
7 a second memory segment for storing a program for decrypting said common  
8 host identifier, authenticating said common host identifier, and determining whether to  
9 send said packet to a second device based on said list and said policy rule;  
10 a processor coupled to said first buffer, said first memory segment and said  
11 second memory segment for executing said program; and  
12 an output means coupled to said first buffer for forwarding said compared data  
13 packet to said second device based on said comparison.

1 22. The apparatus of claim 1, further comprising a second buffer for storing said  
2 compared data packet prior to forwarding said compared data packet to the second  
3 device.

1 23. The apparatus of claim 22, wherein said random access memory comprises  
2 dynamic random access memory.

1 24. The apparatus of claim 23, further comprising a non-volatile random access  
2 memory for storing parameters used by said operating system program.

1 25. The apparatus of claim 24, further comprising means for receiving an updated  
2 list of origination addresses.

1 26. The apparatus of claim 25, wherein said means for receiving comprises an  
2 asynchronous terminal device and a serial port coupled to said dynamic random access  
3 memory.

1 27. The apparatus of claim 25, wherein said means for receiving comprises a  
2 network interface card coupled to said dynamic random access memory.

1 28. The apparatus of claim 21, wherein said first network is a wireless network,  
2 and said input means comprises means for receiving said data packets from said  
3 wireless network.

1 29. A distributed firewall system, comprising:  
2 a first network device;  
3 a second network device in communication with said first network device;  
4 a packet filter processor for each network device;  
5 an encryption means coupled to said packet filter processor, said encryption  
6 means for decrypting and authenticating a packet sent between said first network  
7 device and said second network device; and  
8 a system management module to manage said packet filter processors.

Add  
A2